

REMARKS

In the Office Action, the Examiner rejected claims 1-55. The Applicant requests reconsideration of claims 1-55 in view of the following remarks. No claims are presently added or amended. Accordingly, original claims 1-55 remain pending in the Application.

Objection to the Specification

In the Office Action, the Examiner objected to certain informalities in the specification. Specifically, the Examiner indicated that certain reference numbers should be changed to correspond with the figures. As set forth above, the Examiner's suggestions have been implemented by amending the specification to correct the clerical errors. Accordingly, the Applicant asserts that appropriate corrections have been made and requests that the Examiner withdraw the objection to the specification.

Objection to the Drawings

In the Office Action, the Examiner objected to the drawings because "paragraph [022] refers to a login token but no reference to a login token is made in Fig. 3A." Office Action, page 2. The Applicant respectfully disagrees. Indeed, the Applicant asserts that a login token is clearly illustrated in Fig. 3A as login cookie 300. The paragraph cited by the Examiner, paragraph [022], indicates that the login cookie 300 is a specific type of login token. In other words, the login cookie 300 is a species of login token. Thus, the inclusion of the login cookie 300 in Fig. 3A is sufficient to illustrate a login token and the drawings do not require correction. Accordingly, the Applicant respectfully requests withdrawal of the Examiner's objection to the drawings.

Claim Rejections Under 35 U.S.C. § 102

In the Office Action, the Examiner rejected claims 1-8, 11-13, 15-34, and 42-55 under 35 U.S.C. § 102(e) as anticipated by Sandhu et al. (U.S. Patent No. 6,883,095) (“Sandhu reference”). The Applicant respectfully traverses this rejection. Specifically, with regard to the independent claims the Examiner stated:

As per independent claim 1, Sandhu et al. teaches a login method comprising processing a login token, if provided, during a login attempt, wherein the login attempt is impermissible, and thus unsuccessful, if the login attempt occurs before expiration of a first period of time following an unsuccessful login attempt associated with said login token (*note column 10, line 45 – logged-in ticket is a login token processed by a server when presented at a login session; also note column 6, lines 54-66 – first period of time described*); and

providing an updated login token in response to the login attempt, wherein the updated login token does not permit a subsequent login attempt before expiration of a second period of time if the login attempt is unsuccessful (*note column 60 – second challenge is the updated login token*).

...

As per independent claim 44, Sandhu et al. teaches a login method comprising processing a login attempt to determine whether the login attempt is successful, said login attempt being successful if permissible and submitted with a valid user name and password combination (*note column 10, line 17 and lines 47-50*);

providing a first-class login token if the login attempt is unsuccessful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay between each of said unsuccessful login attempts (*note column 6, lines 2-3 – first challenge equates to first class login; also note column 13, line 54 – indication field can include data that may allow the user with subsequent login attempt without immediately going to the second challenge*);

providing a second-class login token if the login attempt is unsuccessful and a login token submitted with the login request is second-class, wherein a subsequent login attempt made with said second-class login token is not permissible if submitted prior to expiration of a second time delay, said second time delay exceeding said first time delay (*note column 6, line 10 – second challenge equates to second class login; also note Fig. 8 and 11*);

providing the second-class login token if the login attempt is unsuccessful and is the last of a series of unsuccessful login attempts associated with a first-class login token, said series including more than the predefined number of

unsuccessful login delay (*note column 6, line 10 - second challenge equates to second class login; also note Fig. 8 and 11; also note column 13, line 54 - indication field can include data that may allow the user with subsequent login attempt for certain threshold count before going to the second challenge*); and

providing the second-class login token if a login token is not submitted with the login attempt, said login attempt not being permissible (*note column 10, lines 47-50 - the function performed in the absence of logged-in ticket is described*).

...

As per independent claim 47, Sandhu et al. teaches a computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism comprising:

instructions for processing a login attempt to determine whether the login attempt is successful, said login attempt being successful if permissible and submitted with a valid user name and password combination (*note column 8, lines 31-41; also note column 9, lines 2-3; also note Fig. 4,5,6 and 7*);

instructions for providing a first-class login token if the login attempt is successful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay between each of said unsuccessful login attempts (*note column 8, lines 31-41; also note column 9, lines 2-3; also note Fig. 4,5,6 and 7*);

instructions for providing a second-class login token if the login attempt is unsuccessful and a login token submitted with the login request is second-class, wherein a subsequent login attempt made with said second-class login token is not permissible if submitted prior to expiration of a second time delay, said second time delay exceeding said first time combination (*note column 8, lines 31-41; also note column 9, lines 2-3; also note Fig. 4,5,6 and 7*);

instructions for providing the second-class login token if the login attempt is unsuccessful and is the last of a series of unsuccessful login attempts associated with a first-class login token, said series including more than the predefined number of unsuccessful login attempts combination (*note column 8, lines 31-41; also note column 9, lines 2-3; also note Fig. 4,5,6 and 7*); and

instructions for providing the second-class login token if a login token is not submitted with the login attempt, said login attempt not being permissible combination (*note column 8, lines 31-41; also note column 9, lines 2-3; also note Fig. 4,5,6 and 7*).

As per independent claim 48, Sandhu et al. teaches a computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism comprising:

instructions for processing a login token, if provided, during an attempt to login, wherein the login attempt is impermissible if the login attempt occurs before expiration of a first period of time following an unsuccessful login attempt associated with said login token (*note Fig. 1, 4, 5, 6 and 7; also note column 9, lines 4-6-software necessary for the invention is described; also note Fig. 2A – box 415 and step 510 perform this function*); and

instructions for providing an updated login token in response to the login attempt, wherein the updated login token does not permit a subsequent login attempt before expiration a second period of time if the login attempt is impermissible token (*note Fig. 1, 4, 5, 6 and 7; also note column 9, lines 4-6-software necessary for the invention is described; also note Fig. 2A – box 415, 420, 425, 430, and 435 perform this function*).

As per independent claim 49, Sandhu et al. teaches a computer system for processing login requests, comprising:

a first-class login server and a second-class login server, said first-class login server and said second-class login server each including a storage unit and a processor, said storage unit configured to store login information, said processor configured to process login requests with reference to said login information (*note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 – second class login server function can be done here; also note column 9, line 20 – additional server that can perform any one of the server classes function is allowable*);

the first-class login server and the second-class login server each configured to process a login attempt to determine whether the login attempt is successful, said login attempt being successful if permissible and submitted with a valid user name and password combination (*note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 – second class login server function can be done here; also note column 9, line 20 – additional server that can perform any one of the server classes function is allowable*);

the first-class login server configured to process login attempts made with a first-class login token and the second-class login server configured to process login attempts made with a second-class login token (*note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 – second class login server function can be done here; also note column 9, line 20 – additional server that can perform any one of the server classes function is allowable*);

the first-class login server and the second-class login server each further configured to provide a first-class login token if the login attempt is successful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay between each of said unsuccessful login attempts (*note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 – second class login server function can be done here; also note column 9, line 20 – additional server that can perform any one of the server classes function is allowable*);

the second-class login server further configured to provide a second-class login token if the login attempt is unsuccessful, wherein a subsequent login attempt made with said second-class login token is impermissible if submitted prior to expiration of a second time delay, said second time delay exceeding said first time delay (*note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 – second class login server function can be done here; also note column 9, line 20 – additional server that can perform any one of the server classes function is allowable*); and the first-class login server further configured to provide a second-class login token if the login attempt is unsuccessful and the login attempt is the last of a series of unsuccessful login attempts associated with a specific first-class login token, said series including more than the predefined number of unsuccessful login attempts (*note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 – second class login server function can be done here; also note column 9, line 20 – additional server that can perform any one of the server classes function is allowable*).

Office Action, pages 3-4, 11-12, and 13-17.

Anticipation under 35 U.S.C. § 102 can be found only if a single reference shows exactly what is claimed. *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 U.S.P.Q. 773 (Fed. Cir. 1985). For a prior art reference to anticipate under 35 U.S.C. § 102, every element of the claimed invention must be identically shown in a single reference. *In re Bond*, 910 F.2d 831, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990). To maintain a proper rejection under 35 U.S.C. § 102, a single reference must teach each and every limitation of the rejected claim. *Atlas Powder v. E.I. du Pont*, 750 F.2d 1569 (Fed. Cir. 1984). Accordingly, the Applicant needs only point to a single element not found in the cited reference to demonstrate that the cited reference fails to anticipate the claimed subject matter.

Turning to the claims, independent claims 1 and 48 recite, *inter alia*, “processing a login token ... wherein the login attempt is impermissible [if it] ... occurs before expiration of a first period of time following an unsuccessful login attempt associated with said login token ... [and] providing an updated login token in response to the login attempt.” Independent

claims 44 and 47 recite, *inter alia*, “providing a first-class login token if the login attempt is successful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay ... [and] providing a second-class login token if the login attempt is unsuccessful and a login token submitted with the login request is second-class.” Additionally, independent claim 49 recites, *inter alia*, “the first-class login server and the second-class login server each further configured to provide a first-class login token if the login attempt is successful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay ... the second-class login server further configured to provide a second-class login token if the login attempt is unsuccessful.”

The Sandhu reference fails to teach each and every feature of the present claims. For example, the Examiner attempted to equate the Sandhu reference’s “logged-in ticket” with the presently recited first-class token or login token. However, in contrast to the presently recited features, the logged-in ticket of the Sandhu reference is apparently a mere indication that a successful login has already been achieved. *See* Sandhu et al., col. 11, line 52 – col. 12, line 17. The logged-in ticket does not affect the login attempt; it is merely a result of authentication (i.e., a successful attempt). *Id.* Indeed, once the logged-in ticket is formed by the user device 30, the logged-in ticket appears to provide *immediate* access to a sponsor station 50 because it indicates that a user is *already* logged in. *Id.* The logged-in ticket does not determine whether a login attempt is impermissible. Further, the logged-in ticket does not permit a predefined number of unsuccessful login attempts. Accordingly, the logged-in ticket is not equivalent to the presently recited first-class token or login token, and the Sandhu reference fails to anticipate each and every feature of the presently recited claims.

Additionally, the Sandhu reference fails to teach providing a second-class login token or an updated login token. In the Office Action, in relation to these claim features, the Examiner merely pointed to the Sandhu reference's disclosure of issuing a second challenge with added complexity when a response to a first challenge is insufficient. This is clearly not equivalent to providing an updated or second-class login token (e.g., a cookie), as set forth in the present claims. The "challenges" of the Sandhu reference are related to prompting a user to enter a user ID and password, not providing a login token. *See* col. 11, lines 21-57. Indeed, the Sandhu reference refers to the procedure relating to the multiple challenges as 'password throttling.' *See* Sandhu, et al., col. 11, lines 38-43. Accordingly, the Sandhu reference fails to anticipate every feature of the present claims.

For the reasons set forth above, the Applicant respectfully requests withdrawal of the rejections under 35 U.S.C. § 102. Specifically, the Applicant requests withdrawal of the rejection under 35 U.S.C. § 102 and an indication of allowance for independent claims 1, 44, 47, 48, 49, and the claims depending therefrom.

Rejections Under 35 U.S.C. § 103

The Examiner rejected claims 9, 10, 14, and 35-41 under 35 U.S.C. § 103(a) as being unpatentable over the Sandhu reference in view of Bachman et al. (U.S. Pat. No. 5,907,621) ("the Bachman reference").

The Applicant respectfully traverses this rejection. The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (PTO Bd. App. 1979). To establish a *prima facie* case, the Examiner must not only show that the combination includes *all* of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the

claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (Bd. Pat. App. & Inter. 1985). The

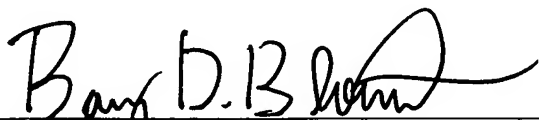
As set forth above, the Examiner relied on the Sandhu reference for its alleged teaching of a first-class token or login token and a second-class login token or an updated login token as recited in each of the independent claims. However, as set forth above, the Sandhu reference fails to anticipate these features of the independent claims. Further, the Bachman reference does not obviate the deficiencies of the Sandhu reference discussed above. In fact, the Examiner does not even suggest that the Bachman reference teaches these features. In view of the deficiencies discussed above with reference to the independent claims, the Applicant respectfully requests withdrawal of the rejection under 35 U.S.C. § 103 and allowance of all pending claims.

Conclusion

In view of the remarks set forth above, the Applicant respectfully requests allowance of claims 1-55. If the Examiner believes that a telephonic interview will help speed this application toward issuance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Date: December 2, 2005



Barry D. Blount
Reg. No. 35,069
FLETCHER YODER
P.O. Box 692289
Houston, TX 77269-2289
(281) 970-4545